UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/864,042	05/22/2001	Viswanath Ananth	5019P001	9969

8791 7590 08/12/2004

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
KIM, JUNG W	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 08/12/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/864,042	**Applicant(s)** ANANTH, VISWANATH	
	Examiner Jung W Kim	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 February 2002* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *10/12/01,07/01/01*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-29 have been examined.

Specification

2. The disclosure is objected to because of the following informalities: on page 5, line 9, an indefinite article is missing. Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 15 is rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections. See MPEP § 2172.01. The omitted structural cooperative relationships are: the structural relationship between the memory (see line 2) and the logic to perform a stream cipher using an encryption key on input data segmented in random sized blocks (see lines 3-4).

Double Patenting

5. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11

F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

6. Claims 1-8, 15-20, 22 and 25 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-8, 12-14, and 17-19 of copending Application No. 09,904,962. Although the conflicting claims are not identical, they are not patentably distinct from each other because both sets of claims define a cipher comprising a routine to divide incoming plain text into variable-sized blocks and a routine converting the plain text into cipher text based on an encryption key and an internal identifier. The additional limitation of an internal state affecting the conversion routine defined in the aforementioned claims of copending Application No. 09,904,962 does not define a patentably distinct limitation since it is an inherent feature of a ciphering device.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 15-17, 20-22 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith et al. U.S. Patent No. 6,243,470 (hereinafter Coppersmith) in view of Ritter U.S. Patent No. 5,727,062 (hereinafter Ritter).

9. As per claim 15, Coppersmith discloses a computing device comprising:

a. a memory (see Coppersmith, Figure 1, Reference No. 28); and

b. logic to perform a stream cipher operation using an encryption key on input data into segmented blocks (see Coppersmith, Abstract).

10. Coppersmith does not expressly disclose the input data as being segmented into random sized blocks. Ritter teaches a cipher wherein the block size is dynamically variable during operation (see Ritter, col. 11, lines 64-67). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Ritter to the cipher of Coppersmith. Motivation for such an implementation, inter alia, include: variable size block ciphers are a better fit to existing systems, better fit to variable size devices and potentially eliminates expansion data. See Ritter, col. 7, lines 28-63; col. 9, lines 5-14. The aforementioned covers claim 15.

11. As per claim 16, Coppersmith discloses a computer device as outlined above in the claim 15 rejection under 35 U.S.C. 103(a). In addition, the stream cipher operation involves encryption. See Coppersmith, Abstract. The aforementioned covers claim 16.

12. As per claim 17, Coppersmith discloses a computer device as outlined above in the claim 15 rejection under 35 U.S.C. 103(a). In addition, the logic is an integrated circuit. See Coppersmith, col. 6, lines 20-24. The aforementioned covers claim 17.

13. As per claims 20 and 24, Coppersmith discloses a computer device as outlined above in the claim 15 rejection under 35 U.S.C. 103(a). In addition, the computing device is a smart card. See Coppersmith, col. 3, lines 37-41. Further, smart cards are secure portable devices, wherein the actuation of the device is restricted to authorized operations. The aforementioned cover claims 20 and 24.

14. As per claim 21, Coppersmith discloses a computer device as outlined above in the claim 15 rejection under 35 U.S.C. 103(a). In addition, the computing device is a node coupled to a network and alternatively a router. See Coppersmith, Figure 2. The aforementioned covers claim 21.

15. As per claim 22, Coppersmith discloses a computer device as outlined above in the claim 15 rejection under 35 U.S.C. 103(a). In addition, the computing device is an operating system. See Coppersmith, Figures 1 and 2, and claim 16.

16. Claims 1-4, 14, 18 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith in view of Ritter, and further in view of Reardon U.S. Patent No. 6,212,635 (hereinafter Reardon).

17. As per claim 1, Coppersmith covers a hybrid cipher operating within a computing device as outlined above in the claim 15 rejection under 35 U.S.C. 103(a). For the reasons outlined above, the cipher comprises:

a. a first software routine to divide incoming plain text into variable-sized blocks (see Coppersmith, col. 7, lines 33-43; col. 7, line 57-col. 8, line 3; see Ritter, col. 11, lines 64-67; col. 7, lines 28-63; col. 9, lines 5-14); and

b. a second software routine to convert the plain text into cipher text based on an encryption key (see Coppersmith, col. 7, line 28-col. 11, line 42).

18. Coppersmith does not expressly teach using an encryption key and an internal identifier to encrypt the plain text. However, use of an identifier in addition to an encryption key to encipher a plain text is a common feature in the art to uniquely associate a cipher text to an encrypting device. For example, Reardon teaches incorporating user and system identification profile information as seed values into a one-way hash function to generate an encryption key. See Reardon, col. 10, lines 40-59. It would be obvious to one of ordinary skill in the art at the time the invention was made for the plain text to be encrypted using an encryption key and an internal identifier

to create a cipher text unique to the device profile as taught by Reardon. Ibid. The aforementioned covers claim 1.

19. As per claims 2 and 3, Coppersmith covers a cipher as outlined above in the claim 1 rejection under 35 U.S.C. 103(a).

20. Coppersmith does not teach generating a value for the block size from a second non-linear function based on the encryption key and the internal identifier. However, as argued above, Coppersmith does teach block size as an adjustable variable and that randomization of block size enables a more secure cipher. See Coppersmith, col. 2, lines 51-53; col. 7, lines 37-38. Further, Ritter teaches block size as a dynamic variable that varies over the course of transmitted data to enable a more adaptable cipher. See Ritter, col. 7, lines 28-63; col. 9, lines 5-14. Moreover, Reardon teaches combining multiple seeds unique to a device (encryption key and internal identifier operate as values unique to an encrypting device) to generate a unique value specific to the device by means of a second non-linear function (a one-way hash function). See Reardon, col. 10, lines 40-59. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the block size to be generated from a second non-linear function seeded with values unique to the cipher device to generate a unique random block size, but deterministic based on values unique to the cipher device as taught by Reardon. Ibid.

21. Further, Coppersmith does not teach using the output of a first non-linear function as a third parameter seed to the second non-linear function to generate the

block size. However, non-linear functions are the basic functions for generating cryptographic pseudo-random variables (as before, one-way hash functions); moreover, the nature of pseudo-random values ensures these values are most likely secure from all attacks except for brute-force methods and hence, effectively secure from unscrupulous third parties. Furthermore, a pseudo-random value as a seed for a non-linear function introduces another randomizing element into the block size generator to make for a more secure encryption system. Examiner takes Official Notice of these teachings. It would be obvious to one of ordinary skill in the art at the time the invention was made for the block size to be further determined based on a first non-linear function since the block size would be based on a pseudo-random value and hence harder to ascertain as known to one of ordinary skill in the art. The aforementioned cover claims 2 and 3.

22. As per claim 4, Coppersmith covers a cipher as outlined above in the claim 1 rejection under 35 U.S.C. 103(a).

23. In addition, the second software routine further performs a first shuffling operation on an internal state of a computing device based on the encryption key so that a single bit modification of the encryption key requires complete recalculation of the internal state of the computing device. See Coppersmith, Figure 5B, Reference No. 610 and related text. The aforementioned covers claim 4.

24. As per claim 14, Coppersmith covers a cipher as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, Coppersmith discloses the use of table lookup to encrypt and decrypt data. See Coppersmith, col. 3, lines 16-20. Further, table lookups that decrypt variable blocks of ciphertext use arrays having data elements that are permuted to correspond to an inverse of an array of an internal state of the computing device that was used to encrypt the original plaintext. The aforementioned covers claim 14.

25. As per claims 18 and 19, they are apparatus claims corresponding to claims 2 and 3, and they do not teach or define above the information claimed in claims 2 and 3. Therefore, claims 18 and 19 are rejected as being unpatentable over Coppersmith in view of Reardon for the same reasons set forth in the rejections of claims 2 and 3.

26. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith in view of Ritter and Reardon, and further in view of Fielder et al. U.S. Patent No. 5,963,646 (hereinafter Fielder).

27. As per claim 5, Coppersmith covers a cipher as outlined above in the claim 4 rejection under 35 U.S.C. 103(a).

28. In addition, as outlined above, Coppersmtih does teach initializing the internal state of the computing device based on at least an internal identifier; but does not teach a second shuffling operation on the internal state of the computing device based on at

least the internal identifier. Fielder teaches shuffling internal identifiers to generate a cipher key, which is used to encrypt a plain text. See Fielder, Figure 2, Reference No. 52. It would be obvious to one of ordinary skill in the art at the time the invention was made for a second software routine to perform a second shuffling operation on the internal state of the computing device based on at least the internal identifier to resist cryptographic analysis. See Fielder, col. 3, lines 1-6. The aforementioned covers claim 5.

29. Claims 6-10 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith in view of Ritter and Reardon, and further in view of Moskowitz et al. U.S. Patent No. 5,822,432 (hereinafter Moskowitz).

30. As per claims 6 and 10, Coppersmith covers a cipher as outlined above in the claim 1 rejection under 35 U.S.C. 103(a).

31. Coppersmith does not disclose a third software routine to determined if a plurality of random data elements are to be distributed within the cipher text and to map the plain text for the insertion of the random data elements. Moskowitz teaches a method of inserting random values into a digital stream (watermarking the data), which are based on human interactive input information, by mapping these values into the digital stream wherein a key is used to identify the locations of the random values. See Moskowitz, claims 1 and 4; Figure 1. It would be obvious to one of ordinary skill in the art at the time the invention was made for the cipher to include a third software routine to

determine if a plurality of random data elements are to be distributed within the cipher text then map the plain text. Motivation for such an implementation enables the cipher to insert a watermark contingent on input by a user. See Moskowitz, col. 2, lines 31-55. The aforementioned cover claims 6 and 10.

32. As per claim 7, Coppersmith covers a cipher as outlined above in the claim 6 rejection under 35 U.S.C. 103(a).

33. In addition, Moskowitz teaches the third software routine determines an amount of random data elements distributed within the cipher text is programmable based on a percentage value entered by a user, or set based on the encryption key and internal identifier and the internal state of the hybrid stream cipher. See Moskowitz, claim 4. It would be obvious to one of ordinary skill in the art at the time the invention was made for the third software routine to determine an amount of random data elements distributed within the cipher text to be programmable based on a percentage value entered by a user to enable the user to minimize the footprint while maximize the security of the watermark. See Moskowitz, col. 1, lines 46-51. The aforementioned covers claim 7.

34. As per claim 8, Coppersmith covers a cipher as outlined above in the claim 6 rejection under 35 U.S.C. 103(a).

35. Coppersmith does not disclose that the amount of random data elements distributed within the cipher text is based on the encryption key, the internal identifier

and the internal state of the hybrid stream cipher. However, Coppersmith does teach randomizing parameters of a cipher to thwart an observer from discovering the original contents of a cipher text. See Coppersmith, col. 2, lines 51-53. Since the randomization must be deterministic to enable an inverse operation, or at least identify the locations of these random data values in the digital stream, the randomization sequence must be based on values corresponding to the known state of the cipher when the amount of random data elements was initially determined. Hence, values such as the encryption key, the internal identifier and the internal state of the computing device are obvious seeds to generate the amount of random data elements to be distributed within the cipher text. It would be obvious to one of ordinary skill in the art at the time the invention was made for the amount of random data elements distributed within the cipher text to be based on the encryption key, the internal identifier and the internal state of the hybrid stream cipher to automatically generate a random but deterministic value as known to one of ordinary skill in the art. The aforementioned covers claim 8.

36. As per claim 9, Coppersmith covers a cipher as outlined above in the claim 6 rejection under 35 U.S.C. 103(a). In addition, a pseudo-random generator generates pseudo-random data elements. The aforementioned covers claim 9.

37. As per claim 25, Coppersmith covers a method as outlined above in the claim 7 rejection under 35 U.S.C. 103(a). In addition, since the method is a symmetric key

cipher, a decryption method utilizes the same key and the results of its own earlier iterations to randomize the transformation of data. See Coppersmith, Abstract; col. 6, lines 46-59. The aforementioned covers claim 25.

38. Claims 11, 12, 13 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith in view of Ritter, Reardon and Moskowitz, and further in view of Schneier Applied Cryptography (hereinafter Schneier).

39. As per claim 11, Coppersmith covers a cipher as outlined above in the claim 6 rejection under 35 U.S.C. 103(a).

40. As mentioned above, the output stream of the cipher is based on a cipher text and a plurality of random data elements (a watermark), but the invention does not disclose a hash digest of a portion of the output stream as one of the elements added to the output stream. However, hash digests are often used to fingerprint digital data to allow for future validation of its authenticity as taught by Schneier. See Schneier, page 31, first paragraph. It would be obvious to one of ordinary skill in the art at the time the invention was made for the output stream to include a hash digest to enable future verification of the authenticity of the digital stream as taught by Schneier. Ibid.

41. Further, Coppersmith does not expressly disclose mixing the hash digest with the cipher text and the plurality of random data. In a different section, Schneier discloses techniques, such as whitening and permuting, to further obfuscate the output of an encryption function. See Schneier, page 367, 1st and 2nd paragraphs; page 275, 'The P-

Box Permutation'. These functions when applied to the output stream comprising the cipher text, the plurality of random data elements and the hash digest, effectively mixes the three components. It would be obvious to one of ordinary skill in the art at the time the invention was made for a third software routine to produce an output stream based on a mixing of the cipher text, a plurality of random data elements and a hash digest of a portion of the output stream to further obfuscate the distinct portions of the output stream as taught by Schneier. Ibid. The aforementioned covers claim 11.

42. As per claims 12 and 13, Coppersmith covers a cipher as outlined above in the claim 11 rejection under 35 U.S.C. 103(a).

43. In addition, as mentioned above, a watermark is distributed in the cipher text; however, Coppersmith does not disclose a digital signature is distributed in the cipher text. Schneier teaches digital signatures as a means to verify the integrity of a digital stream. See Schneier, page 35, 5 characteristics of a digital signature. It would be obvious to one of ordinary skill in the art at the time the invention was made to distribute a digital signature in the cipher text in order to detect modification. See Schneier, page 35, 4th characteristic of a digital signature. The aforementioned cover claims 12 and 13.

44. As per claim 26, Coppersmith covers a cipher as outlined above in the claim 12 and 25 rejections under 35 U.S.C. 103(a).

45. In addition, a method incorporating a digital signature as a secure addition to transmitted digital data would include steps to verify the digital signature upon reception

of the digital data and take measures dependent on the success or failure of the verification of the digital signature. It would be obvious to one of ordinary skill in the art at the time the invention was made to verify a digital signature of a distributed cipher text and abort decryption if verification fails to ensure restricted digital content can only be read by authorized users as known to one of ordinary skill in the art. The aforementioned covers claim 26.

46. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith.

47. As per claim 23, Coppersmith discloses a computing device as outlined above in the claim 15 rejection under 35 U.S.C. 103(a).

48. Coppersmith does not teach the computing device as a wireless device. However, wireless connectivity between computing devices are well-known network implementations in the art. In particular, the IEEE 802.11 protocol is the standard in which wireless computing devices share the same frequency and space. It would be obvious to one of ordinary skill in the art at the time the invention was made for the computing device to be a wireless device since this enables devices the flexible to be mobile as known to one of ordinary skill in the art. The aforementioned covers claim 23.

49. Claims 27-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith in view of Ritter, Reardon, Moskowitz and Schneier, and further in view of Ginter et al. U.S. Patent No. 5,892,900 (hereinafter Ginter).

50. As per claims 27-29, Coppersmith covers a cipher as outlined above in the claim 26 rejection under 35 U.S.C. 103(a). Coppersmith does not expressly disclose a mechanism for securely selling digital content that uses the cipher as outlined above. Ginter teaches a mechanism for securely selling digital content comprising:

a. assigning a unique internal identifier to each user (see Ginter, col. 22, lines 1-3);

b. receiving a request from a user for a download of the digital content (see Ginter, Figure 54 and related text);

c. encrypting the digital content and transmitting the encrypted digital content to the user (see Ginter, col. 12, lines 31-38);

e. wherein the mechanism includes a copyright in one of a plain text form, an image or an icon to operate as a digital signature, that is needed for decrypting the digital content and allowing the digital content to be uniquely sold to a particular user, and wherein the digital content is software that is placed on a removable media or downloaded on-line (see Ginter, col. 8, lines 1-3; col. 12, lines 31-44; col. 22, lines 5-8; col. 202, line 40-col. 205, line 19, 'Fingerprinting').

51. It would be obvious to one of ordinary skill in the art at the time the invention was made for the cipher covered by Coppersmith to be implemented in a mechanism for

securely selling digital content as disclosed by Ginter to enable secure distribution and handling of electronic proprietary content. See Ginter, col. 1, lines 8-30; col. 2, lines 32-56. The aforementioned cover claims 27-29.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Coppersmith et al. U.S. Patent No. 6,192,129.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
August 2, 2004

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100